SAMI
ADVANCED
ELECTRONICS
شركة الإلكترونيات المتقدمة

SAMI-AEC Cybersecurity Solutions

SAMI-AEC Cybersecurity Solutions

CONTENTS

SAMI-AEC Cybersecurity Solutions

As a leading provider of security products and solutions, SAMI-AEC follows a prudent, effective, and infallible approach to providing cybersecurity solutions to organizations. SAMI-AEC comprehensive and integrated set of offerings including Cyber Range, Data Diode, Security Operations Center (SOC) and SIEM which helps in strengthening the security posture of organizations. Besides, these offerings focus on protecting the mission-critical infrastructure of national industries such as defense, energy, finance, transport, etc.

SAMI-AEC indigenously developed cybersecurity solutions add a layer of added security by nurturing cyber readiness across organizations. This in turn helps these organizations in staying aware of real-world scenarios and cyber threats, prompting them to make swift and timely action to prevent any cyberattacks or data breaches.

Cyber Range

SAMI-AEC Cyber Range delivers realistic simulation environment to assess, develop and maintain cyber readiness. AEC Cyber Range offers “real world” functions, the same way as the real internet but in a fully controlled environment.

Introducing the SAMI-AEC Cyber Range powered by Coliseum®

SAMI-AEC Cyber Range is a cybersecurity training and exercises platform, enabling to develop and conduct light-touch and/or custom exercises, based on the IT or OT environment known by our customers. SAMI-AEC cyber range offers realistic and automated scenario development options and to create and execute continuous online, organization-wide cybersecurity training & awareness programs to inflict collective change of behavior for crisis avoidance and management, and thus, ultimately, achieve cyber resilience.

Cyber attack will happen at your organization. The question is: are you prepared?

Exercise with real life cyber threats:

SAMI-AEC cyber range provides scenarios replicating real life cyber threats, tools and tactics used by adversaries. This way the blue team and the organization can gain the hands-on experience of the impact of a cyber attack and assess its incident response capabilities.

Cyber Exercises

> The ability to learn faster is your only sustainable advantage

Cyber wargames and exercises

Experience the power of custom planned highly engaging tailored cyber wargames and exercises delivered in a cyber range environment realistically simulating networks and infrastructure familiar to the participants.

Decision making under pressure

- Respond to real-world cyberthreats in a realistic environment
- Experience the high-pressure situations with real-world cyber attacks
- Validate incident response plans
- The effect of rapid decisions
- Experience the impact of an incident & costs

Experience team cohesion

- Cross-organizational, cross-sectoral, multinational scenarios
- Validate organizational cyber resilience
- Test communication and media plans
- Identify individual and team cyber competence strengths and weaknesses

Technical evaluation, testing and development

- Incidents happen at the joint where various IT solutions and humans meet. Validate and test current and future infrastructure elements and systems against real-world cyber threats
- Build digital and cyber dexterity through experiencing before implementing solutions

SAMI-AEC Data Diode

Data Diodes are designed to protect highly sensitive data and networks in industries, e.g., military and aerospace, oil and gas, and utilities, e.g., water and electricity, and other critical infrastructure.

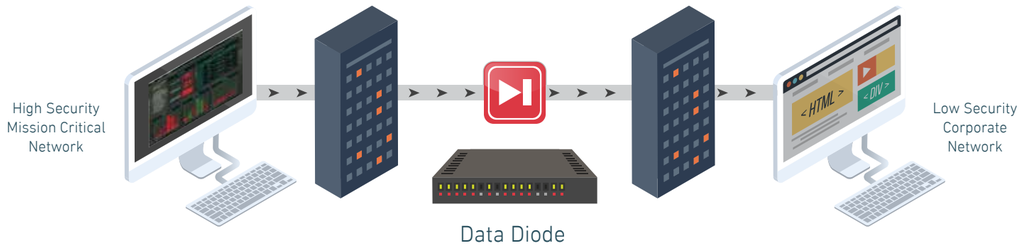
Data diodes enhance security by physically limiting the flow of data in one direction on a hardware level. A common practice is to completely disconnect the network from other networks. These disconnected networks are referred to as isolated or air-gapped networks. This has been the use case for numerous critical infrastructure and SCADA systems, as well as military networks. This infrastructure becomes more problematic with the growing need to import and export data from isolated networks. The manual transfer of data generates further security risk and increases human workload, making data transfer prone to human error. This is where data diodes truly shine. A data diode solves these issues by providing a physically secure “one-way” communication channel from an unsecure network to the secure network (or vice-versa). The one-way channel allows data to be safely transferred to the secure network, while not allowing any data to leave it.

Data diodes ensure the following

Prevent hackers from penetrating the secure network

Provide 100% data leak prevention, since no data can leave the network due to physical restrictions

Data Diode Connectivity Diagram



Data Diode Features

Data diodes support a wide range of data formats, including: SCADA systems, SoC systems logs, programmable logic controller (PLCs), historians, patches management and sensors, and other Industrial Control Systems (ICSs) located on the operation technology (OT) network.

The SAMI-AEC Data Diode currently supports the following protocols:

1. Syslog
2. FTP
3. SFTP
4. SCP
5. Raw TCP
6. Raw UDP
7. PI

We are considering the below protocols/applications for our future development:

- SMTP
- Modbus
- SNMP
- Modbus
- Netflow
- Others

Security Operations Center (SOC)

The SAMI-AEC SOC located in SAMI-AEC Headquarters in Riyadh is capable of monitoring, detecting, and isolating security-related incidents and the security management of the organization's security products, network devices, servers, security systems, and IT Data Center. The SOC services offered are in compliance with Saudi National Cybersecurity Authorities regulation.

SAMI-AEC offers multiple service delivery models tailored to customer needs. Offsite models utilize a secure channel between the SOC and Client Premises. SIEM administration can be onsite/offsite as needed.

SAMI-AEC SOC Team are 100% Saudi Nationals who are highly experienced in handling security incidents and have expert skills working with leading SIEM Solutions such as LogRhythm, QRadar, RSA, Splunk, and ArcSight. Our SOC analysts are trained to work with advanced Security Solutions and in executing below offerings

Benefits

- No Need to Hire, Manage and Train Resources
- SLA Commitment to keep the customers satisfied
- Flexible and Adaptive
- Utilize Back-office Resources when required
- Letting Organizations Focus on their Core Strength
- Cost Optimization (Shared Resources; Offshore)
- Simplified Accountability
- SAMI-AEC Strong Partnership means strong support from vendors

Offering

Governance

- Create/Review SOC Playbook (policies, procedures)
- Assessment & Remediation

SIEM Management

- Managing and Administering SIEM Solutions
- Periodic and Continuous Fine tuning of Use Cases

Digital Forensics and Incident response

- RCA for incidents
- Data Recovery and Analysis
- Malware Analysis to understand the behavior and purpose of a suspicious file or URL.

Log Analysis and Monitoring

- 24x7x365 monitoring for malicious activities, network traffic, endpoints, logs and security events
- Advanced Log and Vulnerability Management
- Incident Ticketing and Workflow Management

Metrics and Reporting

- Well defined and meaningful KPIs, KRAs
- Easy to setup and use search and alert features
- Highly configurable reports and dashboards

Training and Certifications

- Certified SOC Analyst Training (CSA)
- Cyber Security Certifications
- SIEM Training (Vendor specific)
- OTJ Trainings

Threat Intelligence

- Scoring and prioritization to ensure your threat intelligence is relevant
- Aggregate, correlate, and analyze threat data from multiple sources in real time to support defensive actions.
- Continuous Threat Hunting and Analysis

Security Information and Event Management (SIEM)

Security information and event management (SIEM) products combine security information management (SIM) and security event management (SEM). They provide real-time analysis of security alerts generated by applications, servers and network devices

SAMI-AEC SIEM has multiple capabilities including gathering, analyzing and presenting information from network and security devices, database and application logs, as well as providing sandboxing capabilities that is used to execute untested or untrusted programs, files, and URLs from unverified or untrusted third sources without exposing harm to the host machine

System Functionalities

Log Management
Collects and stores log files from multiple hosts and systems into a centralized single location instead of accessing them from each system individually

Sandbox
Executes files and URLs, inline or on-demand, in an isolated environment to protect users from zero-day. It examines the behavior of the files and URLs, and reports the result of the analysis

Network Forensics
Provides an after-the-fact investigative capability that other security tools cannot provide. Use cases include capturing malware samples, network exploits and determining if data exfiltration has occurred

Incident Response
Provide the functionality of generating tickets based on security alerts, by the system or customized use cases, in order to enable Incident Response team to investigate alerts and respond to verified breaches

Threat Intelligence
Enables the SIEM to recognize the emerging attack campaigns and new trends. The primary objective of threat Intel in to detect Advanced Persistent Threats (APT) and zero-days attack

SAMI
ADVANCED
ELECTRONICS
شركة الإلكترونيات المتقدمة

SAMI Advanced Electronics Company
P.O. Box 90916,
King Khalid International Airport, Industrial Estate
Riyadh 11623, Saudi Arabia
Tel : +966 11 220 1350
Fax : +966 11 220 1355
Email: info@aecl.com
Web: www.aecl.com
AECSaudiArabia

SAMI
ADVANCED
ELECTRONICS
شركة الإلكترونيات المتقدمة

نظام المعلومات الأمنية وإدارة الأحداث

منتجات نظام المعلومات الأمنية وإدارة الأحداث تجمع ما بين إدارة أمن المعلومات وإدارة الأحداث الأمنية، وتوفر تحليلاً آنيّاً للتنبيهات الأمنية الناتجة عن الخوادم وأجهزة الشبكة

إن نظام المعلومات الأمنية وإدارة الأحداث من شركة الإلكترونيات المُتقدّمة لديه القُدرة على جمع وتحليل وتقديم المعلومات من أجهزة الشبكة وقاعدة البيانات والتطبيقات. ويحتوي النظام أيضاً على تقنية صندوق الرمل، وهي تقنية مفيدة للغاية عند الحاجة لتشغيل بعض البرامج المشكوك بها، حيث يمكن تشغيلها وتجربتها في إطار محدود، دون أن تتمكن من تدمير أو التلاعب في ملفات الجهاز، ممّا يوفر حماية أكبر لباقي البرامج.

وظائف النظام

إدارة السجل

يجمع ويخزن ملفات السجل من أنظمة متعددة في موقع واحد مركزي بدلاً من الوصول إليها من كل نظام على حدة

تقنية صندوق الرمل

هي تقنية مفيدة للغاية عند الرغبة في تشغيل بعض البرامج المشكوك بها، حيث يمكن تشغيلها وتجربتها في إطار محدود، دون أن تتمكن من تدمير أو التلاعب في ملفات الجهاز، مما يوفر حماية أكبر لباقي البرامج

التحاليل الجنائية للشبكة

يوفر القدرة على التحقيق في الحالات التي يُمكن لبعض أجهزة الحماية ألّا توفر أدوات كافية للأمان. وتشمل حالات الاستخدام التقاط عينات من البرامج الضارة، والتحقيق فيما إذا كان هناك تسريب للمعلومات

الاستجابة للحادث

توفير خدمة إنشاء تذاكر بناء على تنبيهات الأمان، من قبل النظام أو حالات الاستخدام حسب الطلب، من أجل تمكين فريق الاستجابة للحوادث التحقيق في التنبيهات والرد عليها والانتهاكات التي تم التحقق منها

الطرق الاستخبارية لجمع المعلومات

تمكّن نظام المعلومات الأمنية وإدارة الأحداث من التعرف على حملات الهجوم الناشئة والجديدة. الهدف الأول هو كشف التهديدات المتقدمة والجديدة.

الحلول التي تقدمها شركة الإلكترونيات المُتقدّمة

الحوكمة

- إنشاء ومراجعة دليل العمل في مركز عمليات الأمن السيبراني (السياسات والإجراءات)
- التقييم والمعالجة

إدارة منصة المعلومات الأمنية والأحداث (SIEM)

- الإدارة والإشراف على حلول المعلومات الأمنية وإدارة الأحداث (SIEM)
- تحديث وضبط دوري ومستمر لحالات الاستخدام

التحليل الجنائي الرقمي والاستجابة للأحداث

- تحليل الأسباب الجذرية للأحداث (RCA)
- حلول استعادة البيانات وتحليلها
- تحليل البرامج الضارة لفهم سلوك ملف معين أو عنوان إنترنت (URL) مشبوه والغرض من وجوده

تحليل ومراقبة سجلات الأحداث

- المراقبة على مدار الساعة وطوال أيام السنة للتهديدات المحتملة وحركة مرور البيانات داخل الشبكة بالكامل ونقاط النهاية والسجلات والأحداث السيبرانيه
- إدارة مُتقدّمة للسجلات والثغرات الأمنية
- إدارة سير العمل وتذاكر الحوادث الأمنية السيبرانيه

المعايير وإصدار التقارير

- تعريف وضبط مؤشرات أداء رئيسية (KPIs) ومجالات نتائج رئيسية (KRAs) مُحدّدة بدقّة
- سهولة الإعداد واستخدام ميزات البحث والتنبيه
- تقارير ولوحات معلومات قابلة لتعديلها حسب الحاجة

التدريب والشهادات

- تدريب محلل معتمد (CSA) ل مركز عمليات الأمن السيبراني (SOC)
- شهادات الأمن السيبراني
- التدريب على إدارة المعلومات والأحداث الأمنية (SIEM) – خاص بالموردين
- التدريب أثناء العمل (OJT)

استخبارات التهديدات

- تحديد درجة التهديد وتحديد الأولوية للتأكد من أن استخبارات التهديدات الخاصة بالمُنشأة ذات صلة بالحدث
- القيام بتجميع بيانات التهديد من مصادر متعددة وربطها وتحليلها في الوقت الفعلي لدعم الإجراءات الدفاعية
- اصطياد التهديدات وتحليلها بشكل مستمر

SAMI
ADVANCED
ELECTRONICS
شركة الإلكترونيات المتقدمة

مركز عمليات الأمن السيبراني

مركز عمليات الأمن السيبراني التابع لشركة الإلكترونيات المُتقدّمة والمتواجد داخل المقر الرئيسي للشركة في مدينة الرياض قادر على مراقبة واكتشاف وعزل التهديدات المُتعلّقة بالأمن السيبراني وإدارة المنتجات الأمنية للمُنشأة وأجهزة الشبكة والخوادم وأنظمة الأمان ومركز بيانات تقنية المعلومات. تتوافق الخدمات المُقدّمة من قِبَل مركز عمليات الأمن السيبراني (SOC) مع تعليمات وأنظمة الهيئة الوطنية للأمن السيبراني السعودية.

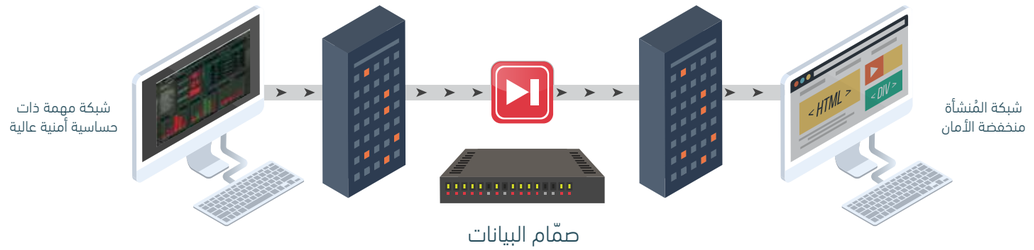
تقدم شركة الإلكترونيات المُتقدّمة نماذج وطرق عمل متعددة للخدمات مُصمّمة خصيصاً للتناسب مع احتياج العملاء. تستخدم النماذج العاملة خارج الموقع (عن بعد) قناة اتصال آمنة بين مركز عمليات الأمن السيبراني وموقع العميل. كما يمكن أن تكون منصة إدارة المعلومات الأمنية والأحداث (SIEM) في الموقع أو خارج الموقع حسب الحاجة.

إن الفريق العامل في مركز عمليات الأمن السيبراني في شركة الإلكترونيات المُتقدّمة هو فريق سعودي بالكامل وتمتع كوادره المختلفة بخبرات واعتمادات مُتقدّمة في التعامل مع التهديدات الأمنية ولديهم المهارات اللازمة كخبراء في العمل على الحلول الرائدة في إدارة المعلومات الأمنية والأحداث (SIEM) مثل حلول LogRhythm وQRadar وRSA وSplunk وArcSight. حيث يتم تدريب محللي مركز عمليات الأمن السيبراني لدينا على العمل مع حلول الأمن السيبراني المتقدمة هذه لتحقيق وتنفيذ ما نعرضه أدناه

الفوائد

- لا حاجة لتوظيف وإدارة وتدريب موظفين مختصين
- تتميز بالمرونة والقابلية العالية للتكيف
- السماح للمُنشآت بالتركيز على نقاط قوتها وأعمالها الجوهرية
- تسهيل تحمل المسؤوليات
- الالتزام باتفاقيات مستوى الخدمة (SLA) من أجل الحفاظ على رضا العملاء
- استخدم موارد مكتب المُساندة عند الحاجة
- تمكين الاستفادة من التكلفة المدفوعة عن طريق (المُشاركة في الموارد؛ نقل العمليات إلى الخارج)
- الشراكة القوية مع شركة الإلكترونيات المُتقدّمة تعني دعماً قوياً من الموردين

مخطط توصيل صمّام البيانات



مزايا صمّام البيانات

تدعم صمّامات البيانات مجموعة واسعة من صيغ البيانات، بما في ذلك: أنظمة SCADA، وأنظمة مركز التشغيل للأمن السيبراني ووحدات التحكم المنطقية القابلة للبرمجة (PLCs)، البيانات التاريخية، وتحديث البيانات والأنظمة وأجهزة الاستشعار، وغيرها من أنظمة التحكم الصناعي (ICSs) الموجودة على شبكات تقنيات التشغيل (OT).

حالياً، يدعم صمّام البيانات من شركة الإلكترونيات المُتقدّمة البروتوكولات التالية:

1. Syslog
2. FTP
3. SFTP
4. SCP
5. Raw TCP
6. Raw UDP
7. PI

وفي إطار التطوير المستمر، نعمل على تغطية البروتوكولات\والتطبيقات التالية مستقبلاً:

- SMTP
- SNMP
- Netflow
- Modbus
- Modbus
- وغيرها من البروتوكولات

صمّام البيانات

إن الهدف الرئيسي وراء تصميم واستخدام صمّام البيانات هو توفير أقصى درجات الحماية للبيانات والشبكات الحساسة والمعزولة في قطاعات معينة، مثل القطاع العسكري، وقطاعي النفط والغاز، والمرافق الحسّاسة كقطاعات المياه والكهرباء وغيرها من قطاعات البُنية التحتية الهامة الأخرى.

تعمل صمّامات البيانات على تحسين مستوى الأمان عن طريق الحد من تدفق البيانات ليقتصر التدفق على أن يكون في اتجاه واحد على مستوى الأجهزة. وبشكل عام، يؤدي استخدام صمّام البيانات إلى فصل الشبكة تماماً عن الشبكات الأخرى. ويُشار عادة إلى هذه الشبكات غير المتصلة، بالشبكات المعزولة تماماً Air gapped. هذا هو الحال بالنسبة للعديد من شبكات البُنى التحتية الحيوية وأنظمة SCADA، وكذلك الشبكات ذات الاستخدام العسكري. حيث تصبح هذه البُنى التحتية مُعرضة أكثر للمخاطر مع تنامي حاجتها لاستيراد وتصدير البيانات من الشبكات المعزولة. إن النقل اليدوي للبيانات يؤدي إلى مزيد من المخاطر الأمنية ويزيد العبء على الأفراد العاملين في هذا المجال، ممّا يجعل نقل البيانات عرضة بشكل دائم للخطأ البشري. هنا يأتي الدور الهام الذي يقوم به صمّام البيانات. يقوم صمّام البيانات بحل هذه المشكلات من خلال توفير قناة اتصال "أحادية الاتجاه" آمنة مادياً لنقل البيانات من شبكة غير آمنة إلى الشبكة الآمنة (أو العكس) بحيث تسمح القناة أحادية الاتجاه بالنقل الآمن للبيانات إلى الشبكة الآمنة، مع عدم السماح بترك أي بيانات لا يتم نقلها.

يضمن استخدام صمّام البيانات

منع المتسللين من اختراق الشبكة الآمنة

منع تسرب البيانات بنسبة 100%، حيث لا يمكن لأي بيانات مغادرة الشبكة بسبب القيود المادية التي يفرضها صمّام البيانات

عمليات المحاكاة للهجمات السيبرانية

تعد القدرة على التعلُّم السريع أهم الميزات المستدامة لديك

المناورات وعمليات المحاكاة السيبرانية

تعرَّف على قوة المناورات والتمارين والمحاكاة السيبرانية المُخطَّطة مُسبقاً والمُخصَّصة بحسب احتياج العميل والتي يتم توفيرها في بيئة نطاق سيبراني بهدف محاكاة البيئة الواقعية للشبكات والبنية التحتية المألوفة للمشاركين.

اتخاذ القرار تحت الضغط

- الاستجابة للتهديدات السيبرانية الحقيقية في بيئة واقعية
- التدرب على التعامل مع الحالات المماثلة تحت ضغوط كبيرة ناتجة عن الهجمات السيبرانية التي تحدث في العالم الحقيقي
- التحقق من فاعلية خطط التصدي والتعامل مع تلك الحوادث
- قياس تأثير اتخاذ القرارات السريعة
- التعرُّف على الآثار الجانبية للحوادث وتكاليف إصلاحها

التعرُّف على قوة تماسك الفريق

- تقديم تصورات لحلول واقعية بين مختلف أقسام المنشأة ولعدة قطاعات وبين جنسيات مختلفة
- التحقق من قدرة الصمود السيبراني للمُنشأة
- اختبار خطط التواصل والإعلام
- تحديد نقاط القوة والضعف في كفاءة التعامل مع الهجمات السيبرانية على المستويين الفردي والجماعي

التقييم الفني والاختبار والتطوير

- تحدث الهجمات السيبرانية في مكان التقاء حلول تقنية المعلومات على اختلافها مع البشر. لذلك، من الضروري أن يتم التحقق ومراجعة عناصر وأنظمة البنية التحتية الحالية والمستقبلية وإجراء الاختبارات عليها ضد التهديدات السيبرانية في العالم الحقيقي
- بناء المهارات الرقمية والسيبرانية من خلال تجربة حدوث الهجمات قبل تنفيذ الحلول على أرض الواقع

النطاق السيبراني

يوفر النطاق السيبراني من شركة الإلكترونيات المُتقدّمة بيئة محاكاة واقعية لتقييم الجاهزية السيبرانية للمُنشأة وتطويرها والحفاظ عليها. كما يتيح النطاق السيبراني إمكانية أداء مهام "العالم الحقيقي"، بنفس الطريقة التي يقوم بها الإنترنت الحقيقي، ولكن في بيئة يتم مراقبتها بشكل كامل.

نقدم النطاق السيبراني من شركة الإلكترونيات المُتقدّمة بدعم من Coliseum®

النطاق السيبراني هو عبارة عن منصة للتدريب والتمرين على عمليات الأمن السيبراني. حيث تُمكِّن هذه المنصة المتدربين من تطوير وإجراء تمارين مُبسّطة أو مُخصَّصة على حسب الحاجة، وذلك اعتمادًا على بيئة تقنية المعلومات أو التقنيات التشغيلية التي يستخدمها عملاؤنا. يوفر النطاق السيبراني من شركة الإلكترونيات المُتقدّمة خيارات عديدة لتطوير سيناريوهات واقعية وآلية لإنشاء وتنفيذ برامج تدريب وتوعية مستمرة في مجال الأمن السيبراني على مستوى المُنشأة، ممّا يُساعد في إحداث تغيير جماعي في السلوك لتجنب الأزمات وإدارتها، وبالتالي تحقيق المرونة السيبرانية المطلوبة في نهاية المطاف.

ربما ستتعرض منشأتك للهجمات السيبرانية في يوم من الأيام. والسؤال هنا: هل أنتم مستعدون لمواجهة تلك الهجمات؟

التدريب على مواجهة التهديدات السيبرانية الواقعية:

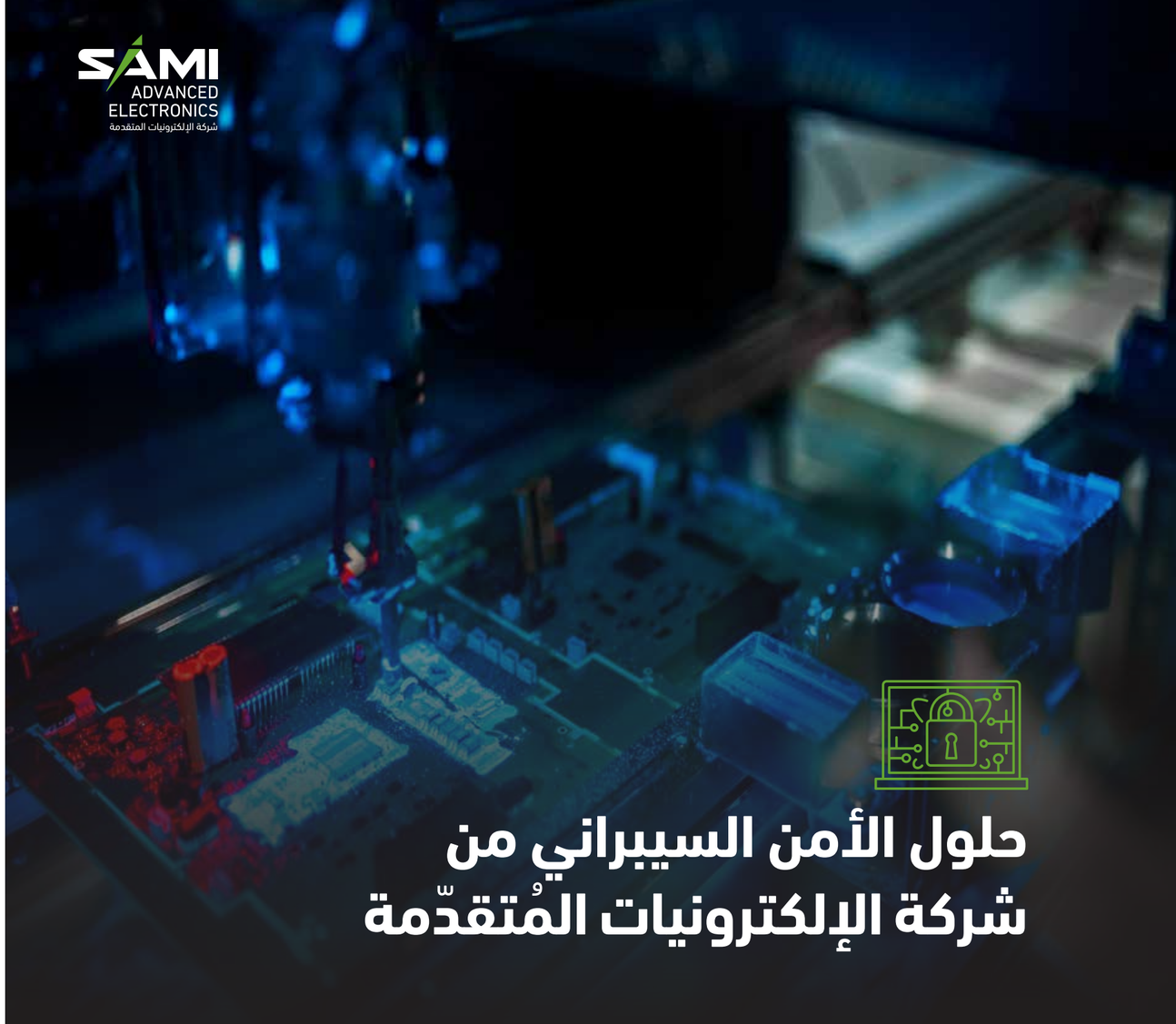
يُقدّم النطاق السيبراني لشركة الإلكترونيات المُتقدّمة سيناريوهات لحالات تكرار التهديدات السيبرانية التي تحدث فعليًا على أرض الواقع بالإضافة للأدوات والتكتيكات التي يستخدمها الأعداء. بهذه الطريقة يمكن للفريق التقني المسئول عن مراقبة أمن المعلومات للمُنشأة أن يكتسب خبرة عملية من خلال تأثيرات الهجوم السيبراني وتقييم قدرات الاستجابة والتعامل مع مثل هذه الحوادث.

حلول الأمن السيبراني من شركة الإلكترونيات المُتقدّمة

بصفتها مزوداً رائداً للمنتجات والحلول الأمنية، تتبع شركة الإلكترونيات المُتقدّمة نهجاً رشيداً وفعالاً وصائباً من أجل توفير حلول الأمن السيبراني للمُنشآت. تشمل مجموعة المنتجات الشاملة والمتكاملة التي تقدمها شركة الإلكترونيات المُتقدّمة النطاق السيبراني، وصمام البيانات، ومركز العمليات الأمنية (SOC)، ونظام إدارة المعلومات والأحداث الأمنية (SIEM)، الذي يساعد في تعزيز الوضع الأمني للمنظمات. بالإضافة على ذلك، تركز هذه المنتجات على حماية البنية التحتية للصناعات الوطنية ذات المهام الحسّاسة مثل الصناعات الدفاعية والطاقة والتمويل والنقل وما إلى ذلك.

تضيف حلول الأمن السيبراني المطورة محلياً من قبل شركة الإلكترونيات المُتقدّمة طبقة إضافية من الأمان السيبراني من خلال تعزيز الجاهزية الإلكترونية للمُنشآت. وهذا بدوره يساعد هذه المُنشآت في البقاء على دراية تامة بسيناريوهات التهديدات السيبرانية في العالم الحقيقي، ممّا يدفعهم إلى اتخاذ إجراءات سريعة وفي الوقت المناسب لمنع أي هجمات إلكترونية أو انتهاكات للبيانات.

المحتويات



حلول الأمن السيبراني من شركة الإلكترونيات المُتقدّمة

SAMI
ADVANCED
ELECTRONICS
شركة الإلكترونيات المتقدمة

حلول الأمن السيبراني

من شركة الإلكترونيات المُتقدّمة